James E. Cecchi
CARELLA, BYRNE, CECCHI,
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700

[Additional Attorneys on Signature Page]

Attorney for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ANTHONY DIPAOLA, KEANNA COLE, PEGGY RODRIGUEZ, INDEA SANCHEZ, and ANGELINA ALVARADO SCOTT, Individually And On Behalf Of All Others Similarly Situated, Plaintiffs, v. SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Civil Action No. _____ **COMPLAINT AND** **DEMAND FOR JURY TRIAL**

Plaintiffs Anthony Dipaola, Keanna Cole, Peggy Rodriguez, Indea Sanchez, and Angelina Alvarado Scott ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action against Samsung Electronics America, Inc. ("Samsung" or the "Defendant"). Plaintiffs make the following allegations, except as to allegations specifically pertaining to Plaintiffs, upon information and belief based on, among other things, the investigation of counsel, and review of public documents.

I. NATURE OF THE ACTION

1. Plaintiffs bring this action against Samsung because it failed to protect the sensitive

and confidential Personally Identifiable Information ("PII") of millions of customers—including first and last names, dates of birth, postal addresses, precise geolocation data, email addresses, and telephone numbers. Defendant's wrongful disclosure has harmed Plaintiffs and the Class, which includes millions of people.

II. JURISDICTION AND VENUE

2. This Court has jurisdiction over this action under 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and is a class action in which there are more than 1,000 members of the Class, members of the Class (as defined below) are citizens of states different from Defendants, and greater than two-thirds of the members of the Class reside in states other than the states in which Defendant is a citizen.

3. This Court has personal jurisdiction over Defendant because it is headquartered in New Jersey; the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues; and Defendant has intentionally availed itself of this jurisdiction by marketing and selling its products and services in New Jersey.

4. Venue is proper in this District under (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to Plaintiffs' claims occurred in New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

III. PARTIES

A. Plaintiffs

5. Plaintiff Anthony DiPaola ("Plaintiff" for purposes of paragraphs 5 – 12) resides in Bordentown, New Jersey and is a current Samsung customer. Samsung notified Plaintiff DiPaola that Plaintiff's PII was compromised in the Samsung data breach.

6. Plaintiff bought a Samsung Galaxy S21+ smartphone and two Samsung televisions,

which are covered by Samsung's Manufacturer's Warranty. Plaintiff uses applications on Plaintiff's Samsung device(s) to monitor personal and confidential information. Plaintiff also uses Plaintiff's device to view and transact Plaintiff's banking and credit information, make payments, and perform other day-to-day banking activities.

7. Samsung's warranty, as well as any policies governing the operating systems of the products bought by Plaintiff, were presented to him on a take-it-or-leave-it basis, and reading those policies was neither required to use those products, nor were those policies made available to Plaintiff before Plaintiff's purchase of those products.

8. On or about September 2, 2022, Plaintiff DiPaola and the public were first notified of the data breach by Samsung and that cybercriminals had illegally accessed and stolen confidential customer data from millions of Samsung customers' accounts. In addition, Plaintiff DiPaola received an email on September 2, 2022 from Samsung notifying Plaintiff that Plaintiff's Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stole from Samsung's servers.

9. As a direct and proximate result of the breach, Plaintiff DiPaola has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this data breach; discussing the breach with Plaintiff's family; reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud; and freezing Plaintiff's credit report. This is valuable time Plaintiff DiPaola otherwise could have spent on other activities.

10. Plaintiff DiPaola is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. Plaintiff DiPaola has received an increased number of phishing emails and spam telephone calls since July 2022, including notification from

Google that his account was being accessed. Such emails and calls trick consumers into providing sensitive and valuable personal information to scammers and, in turn, increase the risk of Plaintiff suffering from monetary or identity theft. Plaintiff DiPaola has and will spend a great deal of time responding to the effects of the data breach. The time spent dealing with the data breach fallout is time Plaintiff would otherwise have spent on other activities.

11. Plaintiff DiPaola suffered actual injury from having Plaintiff's Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of Plaintiff's Personally Identifiable Information, a form of property that Samsung obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

12. As a result of the data breach, Plaintiff DiPaola anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

13. Plaintiff Keanna Cole ("Plaintiff" for purposes of paragraphs 13 – 20) resides in Grand Rapids, Michigan and is a current Samsung customer. Samsung notified Plaintiff Cole that Plaintiff's PII was compromised in the Samsung data breach.

14. Plaintiff bought a Samsung Galaxy S21 Ultra, Galaxy Note, Galaxy Z Fold4 smartphone and two Samsung televisions, which are covered by Samsung's Manufacturer's Warranty. Plaintiff uses applications on these Samsung devices to monitor personal and confidential health and fitness information. Plaintiff also uses the devices to view and transact Plaintiff's banking and credit information, make payments, and perform other day-to-day banking activity.

15. Samsung's warranty, as well as any policies governing the operating systems of the products bought by Plaintiff, were presented to Plaintiff on a take-it-or-leave-it basis, and reading those policies was neither required to use those products, nor were those policies made available to Plaintiff before Plaintiff's purchase of those products.

16. On or about September 2, 2022, Plaintiff Cole and the public were first notified of the data breach by Samsung and that cybercriminals had illegally accessed and stolen confidential customer data from millions of Samsung customers' accounts. In addition, Plaintiff Cole received an email on September 2, 2022 from Samsung notifying Plaintiff that Plaintiff's Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stolen from Samsung's servers.

17. As a direct and proximate result of the breach, Plaintiff Cole has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this data breach; discussing the breach with Plaintiff's family; reviewing credit reports and reviewing financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time Plaintiff Cole otherwise could have spent on other activities.

18. Plaintiff Cole is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. Plaintiff Cole has received an increased number of phishing emails and spam telephone calls since July 2022, including those informing her to extend her warranties. Such emails and calls trick consumers into providing sensitive and valuable personal information to scammers and, in turn, increase the risk of Plaintiff suffering from monetary or identity theft. Plaintiff Cole has and will spend a great deal of time responding to the effects of the data breach including through observing, monitoring, and working with Credit Karma. The time spent dealing with the data breach fallout is time Plaintiff would otherwise have

spent on other activities.

19. Plaintiff Cole suffered actual injury from having Plaintiff's Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of Plaintiff's Personally Identifiable Information, a form of property that Samsung obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

20. As a result of the data breach, Plaintiff Cole anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

21. Plaintiff Peggy Rodriguez ("Plaintiff" for purposes of paragraphs 21 – 28) resides in Greenwood, Indiana and is a current Samsung customer. Samsung notified Plaintiff Rodriguez that Plaintiff's PII was compromised in the Samsung data breach.

22. Plaintiff bought two Samsung Galaxy S20s, two Galaxy S22s, and a Samsung Galaxy Tab A, which are covered by Samsung's Manufacturer's Warranty. Plaintiff uses applications on these Samsung devices to monitor personal and confidential health information. Plaintiff also uses the devices to view and transact Plaintiff's banking and credit information, make payments, and perform other day-to-day banking activities.

23. Samsung's warranty, as well as any policies governing the operating systems of the products bought by Plaintiff, were presented to Plaintiff on a take-it-or-leave-it basis, and reading those policies was neither required to use those products, nor were those policies made available to Plaintiff before Plaintiff's purchase of those products.

24. On or about September 2, 2022, Plaintiff Rodriguez and the public were first

notified of the data breach by Samsung and that cybercriminals had illegally accessed and stolen confidential customer data from millions of Samsung customers' accounts. In addition, Plaintiff Rodriguez received an email on September 2, 2022 from Samsung notifying Plaintiff that Plaintiff's Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stolen from Samsung's servers.

25. As a direct and proximate result of the breach, Plaintiff Rodriguez has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this data breach; discussing the breach with Plaintiff's family; reviewing credit reports and reviewing financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time Plaintiff Rodriguez otherwise could have spent on other activities.

26. Plaintiff Rodriguez is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. Plaintiff Rodriguez has received an increased number of phishing emails and spam telephone calls since July 2022. Plaintiff has placed a freeze on her credit report and taken additional steps to monitor all banking activity. Such emails and calls trick consumers into providing sensitive and valuable personal information to scammers and, in turn, increase the risk of Plaintiff suffering from monetary or identity theft. Plaintiff Rodriguez has and will spend a great deal of time responding to the effects of the data breach. The time spent dealing with the data breach fallout is time Plaintiff would otherwise have spent on other activities.

27. Plaintiff Rodriguez suffered actual injury from having Plaintiff's Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of Plaintiff's Personally Identifiable Information, a form of property that Samsung obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and

(c) present and increased risk arising from the identity theft and fraud.

28. As a result of the data breach, Plaintiff Rodriguez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

29. Plaintiff Indea Sanchez ("Plaintiff" for purposes of paragraphs 29 – 36) resides in Albuquerque, New Mexico and is a current Samsung customer. Samsung notified Plaintiff Sanchez that Plaintiff's PII was compromised in the Samsung data breach.

30. Plaintiff bought a Samsung Galaxy S20 Ultra FE and Samsung television, which are covered by Samsung's Manufacturer's Warranty. Plaintiff uses applications on these Samsung devices to monitor personal and confidential health information. Plaintiff also uses the devices to view and transact Plaintiff's banking and credit information, make payments, and perform other day-to-day banking activities.

31. Samsung's warranty, as well as any policies governing the operating systems of the products bought by Plaintiff, were presented to Plaintiff on a take-it-or-leave-it basis, and reading those policies was neither required to use those products, nor were those policies made available to Plaintiff before Plaintiff's purchase of those products.

32. On or about September 2, 2022, Plaintiff Sanchez and the public were first notified of the data breach by Samsung and that cybercriminals had illegally accessed and stolen confidential customer data from millions of Samsung customers' accounts. In addition, Plaintiff Sanchez received an email on September 2, 2022 from Samsung notifying Plaintiff that Plaintiff's Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stolen from Samsung's servers.

33. As a direct and proximate result of the breach, Plaintiff Sanchez has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this data breach; discussing the breach with Plaintiff's family; reviewing credit reports and reviewing financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time Plaintiff Sanchez otherwise could have spent on other activities.

34. Plaintiff Sanchez is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. In July 2022, Plaintiff Sanchez was the target and victim of a bank account hack when Plaintiff notice six charges in the amount of $874 from pay-as-you-go phone services. Plaintiff Sanchez reported the fraudulent activity to her bank and continues to monitor her compromised accounts. Plaintiff Sanchez's sensitive and valuable personal information has been provided to scammers and, in turn, increases the risk of Plaintiff suffering another attack from monetary or identity theft. Plaintiff Sanchez has and will spend a great deal of time responding to the effects of the data breach. The time spent dealing with the data breach fallout is time Plaintiff would otherwise have spent on other activities.

35. Plaintiff Sanchez suffered actual injury from having Plaintiff's Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of Plaintiff's Personally Identifiable Information, a form of property that Samsung obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

36. As a result of the data breach, Plaintiff Sanchez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of

identity theft and fraud for years to come.

37. Plaintiff Angelina Alvarado Scott ("Plaintiff" for purposes of paragraphs 37 – 44) resides in Chicago, Illinois and is a current Samsung customer. Samsung notified Plaintiff Scott that Plaintiff's PII was compromised in the Samsung data breach.

38. Plaintiff bought a Samsung Galaxy Tablet S5E, Samsung TV, and Samsung Galaxy Note 10+, which are covered by Samsung's Manufacturer's Warranty. Plaintiff uses applications on these Samsung devices to monitor personal and confidential health information. Plaintiff also uses the devices to view and transact Plaintiff's banking and credit information, make payments, and perform other day-to-day banking activities.

39. Samsung's warranty, as well as any policies governing the operating systems of the products bought by Plaintiff, were presented to Plaintiff on a take-it-or-leave-it basis, and reading those policies was neither required to use those products, nor were those policies made available to Plaintiff before Plaintiff's purchase of those products.

40. On or about September 2, 2022, Plaintiff Scott and the public were first notified of the data breach by Samsung and that cybercriminals had illegally accessed and stolen confidential customer data from millions of Samsung customers' accounts. In addition, Plaintiff Scott received an email on September 2, 2022 from Samsung notifying Plaintiff that Plaintiff's Personally Identifiable Information was among the confidential data that cybercriminals illegally accessed and stolen from Samsung's servers.

41. As a direct and proximate result of the breach, Plaintiff Scott has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this data breach; discussing the breach with Plaintiff's family; reviewing credit reports and reviewing financial account statements for any indication of actual or attempted identity theft or

fraud. This is valuable time Plaintiff Scott otherwise could have spent on other activities.

42. Plaintiff Scott is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. Plaintiff Scott was the target of identity theft, and received a phone call from Affirm informing Plaintiff that Plaintiff was charged $2,500 at Walmart. The purchase occurred at a Walmart in Georgia, while Plaintiff is a resident of Illinois. In response, Plaintiff closed her account and is monitoring statements and credit reports. Plaintiff Scott has and will spend a great deal of time responding to the effects of the data breach. The time spent dealing with the data breach fallout is time Plaintiff would otherwise have spent on other activities.

43. Plaintiff Scott suffered actual injury from having Plaintiff's Personally Identifiable Information compromised as a result of the data breach including, but not limited to (a) damage to and diminution in the value of Plaintiff's Personally Identifiable Information, a form of property that Samsung obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

44. As a result of the data breach, Plaintiff Scott anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the data breach. As a result of the data breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

B. Defendant

45. Samsung is a New York corporation with its American headquarters and principal place of business located at 85 Challenger Road, Ridgefield, New Jersey 07660-2118.

IV. FACTUAL BACKGROUND

46. Samsung is "recognized globally as an industry leader in technology." It has millions of customers, has an estimated brand value of approximately $45.5 billion, and produces

over $200 billion in revenue each year.

47. Samsung manufactures a wide range of consumer and industrial electronic products such as televisions and home appliances (*e.g.*, air conditioners, washer and dryers, stoves, refrigerators and microwave ovens, and so on). Samsung's televisions and home appliances connect to the internet and require customers to create a "Samsung Account" before accessing many of their devices' features.

48. For example, consumers who purchase "smart" televisions typically do so because they want to watch streaming applications, such as Netflix or Hulu, on their televisions rather than on separate devices. Although Samsung advertises that their smart televisions allow owners to have streaming applications at their "fingertips," an owner of a Samsung smart television cannot access those streaming applications without downloading those applications onto their television. But to download those applications, the Samsung smart television owner must create a Samsung Account first.

49. Samsung also produces smartphones, smartwatches, and tablets, and offers applications ("apps") for those devices. Samsung's apps include, but are not limited to, Samsung Health, Samsung Cloud, and Samsung Pay. To access the features of these devices and apps, Samsung requires customers to create a Samsung Account.

50. A "Samsung Account" is the "gateway to the World of Samsung." A Samsung Account allows customers to not only access certain features that improve the usability of the device, but a Samsung Account also provides device-related benefits that only customers with a Samsung Account can access. Those benefits include, but are not limited to, backing up and syncing data, finding a device when it is lost, device support, coupons and discounts, and order tracking.

51. Plaintiffs and other proposed Class Members were required, as current and prospective customers of Samsung, to provide Samsung with sensitive Personally Identifiable Information to purchase or receive Samsung's devices and services.

52. When a customer purchases a Samsung product, creates a Samsung Account, or registers for or uses a Samsung service, the customer may provide Samsung with Personally Identifiable Information such as

- name;
- email address;
- postal address;
- phone number;
- payment card information (including name, card number, expiration date, and security code);
- date of birth;
- gender
- information stored in or associated with the customer's Samsung Account, including the customer's Samsung Account profile, ID, username, and password;
- username and password for participating third-party devices, apps, features, or services;
- information a customer stores on a Samsung device, such as photos, contacts, text logs, touch interactions, settings, and calendar information;
- recordings of a customer's voice when they use voice commands to control a service or contact Samsung's Customer Service team; and
- location data, including (1) the precise geolocation of a customer's device if they

consent to collecting this data and (2) information about nearby Wi-Fi access points and cell towers that may be transmitted to Samsung when the customer uses certain Services.

53. Samsung also collects information automatically from its customers concerning their Samsung devices such as their mobile network operator; connections to other devices; app usage information; device settings; web sites visited; search terms used; the apps, services, or features a customer downloads or purchases; and how and when those services are used.

54. Samsung uses the information that it obtains directly from customers and that it collects automatically to:

- "[O]perate, evaluate, and improve our business, including developing new products and services, managing our communications, analyzing our Services and customer base, conducting market research, aggregating and anonymizing data, performing data analytics, and undertaking accounting, auditing, and other internal functions";
- Communicate with its customers; and
- "[P]rovide ads, which may include targeted (or interest-based) ads delivered on your Samsung device or within certain Samsung-branded apps."

55. The Personally Identifiable Information that Samsung collects from its customers is valuable to Samsung. Indeed, Samsung acknowledges this information "plays a key role in elevating what we do for our community" and that it "engage[s] with [Personally Identifiable Information] to inform and enhance everything from your experience to our communication, and to create and innovate radical solutions that help you overcome barriers."

56. Samsung also knows that its customers value their own Personally Identifiable Information. Samsung acknowledges that its customers "own" their "privacy" and recognizes "the importance [customers] place on the value of [their] privacy."

57. Because Personally Identifiable Information is valuable to Samsung's customers, Samsung made multiple promises to alleviate concerns any customers may have about providing Samsung with this sensitive information.

58. Samsung promised its customers that:

- its devices and services are "designed with privacy and security at top mind";
- it "take[s] data security very seriously";
- it is "committed" to handling its customers' Personally Identifiable Information;
- it "maintain[s] safeguards designed to protect personal information [Samsung] obtain[s]";
- "security and privacy are at the core of what [Samsung] do[es] and what [it] think[s] about every day";
- it has "industry-leading security";
- it "prioritize[s]" protecting customers' Personally Identifiable Information25 through certain security measures; and
- it takes "a holistic approach to security to ensure that, at all levels of the device, [it is] protecting users' security and privacy at all times."

59. Moreover, the Federal Trade Commission ("FTC") has established security guidelines and recommendations for businesses that possess their customers' sensitive Personally Identifiable Information to reduce the likelihood of data breaches like Samsung. Among such recommendations are: limiting the sensitive consumer information kept; encrypting sensitive information sent to third parties or stored on computer networks; and identifying and understanding network vulnerabilities.

60. Thus, Samsung had obligations—created by contract, industry standards, common

law, and its representations to its customers like Plaintiffs and other Class Members—to keep this Personally Identifiable Information confidential and protect it from unauthorized disclosures. Plaintiffs and Class Members provided this Personally Identifiable Information to Samsung with the understanding that Samsung would comply with its representations and its obligations to keep such information confidential and secure from unauthorized disclosures.

61. While Samsung has enriched itself through the collection of a treasure trove of information about Plaintiffs and Class Members, and profited off its collection of that information, Samsung failed to employ reasonable, accepted safety measures to secure that valuable information.

A. The Data Breach

62. On September 2, 2022, the Friday before Labor Day, Samsung released a statement announcing that its "U.S. systems" had been infiltrated "[i]n late July 2022" by "an unauthorized third party" that then stole Personally Identifiable Information that Plaintiffs and other putative Class Members had entrusted to Samsung.

63. According to Samsung, the data breach may have affected customers' Personally Identifiable Information such as name, contact and demographic information, date of birth, and product registration information. Yet Samsung claims "[t]he information affected for each relevant customer may vary."

64. Samsung claims it did not discover the data breach until "[o]n or around August 4, 2022" after an "ongoing investigation."

65. As of September 2, 2022, Samsung was still notifying affected customers of the data breach.

66. Although Samsung touts that it "always aim[s] to do the right thing by being open and honest with [its] customers," Samsung did not release a statement to affected customers until

almost a month after learning of the data breach.

67. Samsung's statement also was not transparent. The statement did not explain how the data breach occurred, how Samsung discovered the data breach, what Samsung systems were affected, why it took over a month for Samsung to reveal the data breach occurred, the number of Samsung customers affected, whether the customers affected were businesses or consumers, what prompted the "ongoing investigation," how long the investigation had been ongoing, or the extent of the Personally Identifiable Information stolen.

68. Chris Clements, Vice President of Solutions Architecture at Cerberus Sentinel, a provider of cybersecurity and compliance services, commented on Samsung's statement announcing the data breach: "The lack of transparency on the number of individuals impacted as well as the delay in notifying them combined with a late Friday holiday weekend release seem like clear attempts to minimize the incident."

69. Plaintiffs and Class Members have been injured by the disclosure of their Personally Identifiable Information in Samsung's data breach.

70. The exposure of Plaintiffs' and Class Members' names, dates of birth, contact, and demographic information, and product registration information increases their risk exponentially for precision spearphishing attacks, engineered SIM swaps, and the threat of credit and loans being taken out in their names.

71. One of the most concerning aspects of the Samsung Data Breach is that the hackers stole "demographic information" from Samsung. Samsung says it collects demographic information to "help deliver the best experience possible with our products and services" (or to target specific advertising to consumers).

72. Samsung's U.S. privacy policy explains this more explicitly: "Ad networks allow

us to target our messaging to users considering demographic data, users' inferred interests, and browsing context. These networks can track users' online activities over time by collecting information through automated means, including through the use of browser cookies, web beacons, pixels, device identifiers, server logs, and other similar technologies."

73. While Samsung has thus far refused to reveal what specific demographic data was stolen, TechCrunch examined Samsung's policies and concluded that this data might include: technical information about your phone or other device, how you use your device, like which apps you have installed and which websites you visit, and how you interact with ads, which are used by advertisers and data brokers to infer information about you. The data can also include your "precise geolocation data," which can be used to identify where you go and who you meet with. Samsung says it collects information about what you watch on its smart TVs, including which channels and programs you've watched.

74. Samsung also says it "may obtain other behavioral and demographic data from trusted third-party data sources," which means Samsung buys data from other companies and combines it with its own stores of customer information to learn more about you, again for targeted advertising. Samsung would not say which companies or data brokers it obtains this data from.

B. Samsung Has a History of Breaches

75. This is not Samsung's first data breach in 2022. Accordingly, Samsung should have been particularly aware of the vulnerability of its security systems.

76. On March 7, 2022, Samsung announced it had suffered a data breach that exposed internal company data, including the source code related to its Galaxy smartphones, algorithms related to Samsung smartphone biometric authentication, bootloader source code to bypass some of Samsung's operating systems controls, source code for Samsung's activation servers, and full source for technology used for authorizing and authenticating Samsung accounts.

77. The company claimed the data breach did not include the personal information of consumers or employees.

78. The incident came to light after Lapsus$, a hacking group, leaked 190GB of Samsung's data to four hundred (400) peers.

79. Following the data breach, Samsung promised it would "implement[] measures to prevent further such incidents and will continue to serve our customers without disruption."

80. It is possible that the data breach that Samsung announced on September 2, 2022 could be a continuation of the March 7, 2022 data breach.

81. "Given the difficulty of completely eliminating malware once it has infiltrated a corporate network, especially one as large and complex as Samsung's, the latest incident could well be a continuation of the March hack," said Chad McDonald, CISO of Radiant Logic, an identity and access management vendor.

82. McDonald further stated: "The fact that they sat on this for as long as they did before they did a public disclosure … implies to me they were less concerned about urgency. This makes me feel like this was quite likely just a continuation of [the former breach] they just hadn't discovered yet."

83. Samsung's repeated security failures reveal that it failed to honor its duties and promises by not, among other things: maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks; adequately protecting Plaintiffs' and the Classes' Personally Identifiable Information; and failing to reasonably limit the sensitive consumer information kept, in violation of FTC recommendations.

V. CLASS ACTION ALLEGATIONS

84. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs

bring this case as a class action on behalf of a Nationwide Class and a Illinois, Indiana, Michigan, New Jersey, and New Mexico Sub-Class, defined as follows:

Nationwide Class

All persons in the United States whose Personally Identifiable Information was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

Illinois Sub-Class

Illinois Sub-Class: All persons in the State of Illinois whose Personally Identifiable Information was maintained on Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

Indiana Sub-Class

Indiana Sub-Class: All persons in the State of Indiana whose Personally Identifiable Information was maintained on Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

Michigan Sub-Class

Michigan Sub-Class: All persons in the State of Michigan whose Personally Identifiable Information was maintained on Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

New Jersey Sub-Class

New Jersey Sub-Class: All persons in the State of New Jersey whose Personally Identifiable Information was maintained on Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

New Mexico Sub-Class

New Mexico Sub-Class: All persons in the State of New Mexico whose Personally Identifiable Information was maintained on Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

85. The Classes are each so numerous that joinder of all members is impracticable. On

information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

86. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant owed Plaintiffs and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Personally Identifiable Information, and whether it breached that duty;

b. Whether Defendant continues to breach duties to Plaintiffs and other Class Members;

c. Whether Defendant's data security systems before the data breach met industry standards;

d. Whether Defendant failed to adequately respond to the data breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay;

e. Whether Plaintiffs and other Class Members' Personally Identifiable Information was compromised in the data breach; and

f. Whether Plaintiffs and other Class Members are entitled to damages as a result of Defendant's conduct.

87. Plaintiffs' claims are typical of the Classes' claims. Plaintiffs suffered the same injury as Class Members—i.e., Plaintiffs' Personally Identifiable Information was compromised in the data breach.

88. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs

has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests that conflict with those of the proposed Classes.

89. Defendant has engaged in a common course of conduct toward Plaintiffs and other Class Members. The common issues arising from this conduct that affect Plaintiffs and other Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

90. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiffs' claims

91. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST COUNT
Negligence
On behalf of Plaintiffs, the Class, and the State Subclasses

92. Plaintiffs re-allege and incorporate by reference all preceding factual allegations found in paragraphs 1 through 91.

93. To access features of the devices, apps, or services Plaintiffs and Class Members purchased, Samsung required Plaintiffs and Class Members to submit non-public Personally Identifiable Information to obtain these features.

94. By collecting and storing this data, and sharing it and using it for commercial gain, Defendant both had a duty of care to use reasonable means to secure and safeguard this Personally Identifiable Information, to prevent disclosure of the information, and to guard the information from theft.

95. Defendant's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

96. Defendant also owed a duty of care to Plaintiffs and members of the Classes to provide security consistent with industry standards and the other requirements discussed and to ensure that its systems and networks—and the personnel responsible for them—adequately protected Defendant's customers' Personally Identifiable Information.

97. Defendant's duty to use reasonable security measures arose as result of the special relationship that existed between it and its customers. Only Defendant could ensure that its systems would protect against the harm to Plaintiffs and the members of the Classes from a data breach.

98. Defendant also had a duty to use reasonable security measures under Section 5 of

the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

99. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law, statutes, and FTC guidance described above, but also because it is bound by, and has committed to comply with, industry standards to protect confidential Personally Identifiable Information.

100. Defendant breached its common law, statutory, and other duties—and thus was negligent—by failing to use reasonable measures to protect its customers' Personally Identifiable Information, and by failing to provide timely notice of the data breach.

101. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Personally Identifiable Information;

b. allowing unauthorized access to Plaintiffs' and Class Members' Personally Identifiable Information;

c. failing to recognize in a timely manner that Plaintiffs' and Class Members' Personally Identifiable Information had been compromised; and

d. failing to warn Plaintiffs and Class Members about the data breach promptly so that they could take appropriate steps to mitigate the potential for identity theft and other damages

102. It was foreseeable that Defendant's failure to use reasonable measures to protect Personally Identifiable Information and to provide timely notice of the data breach would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Classes were reasonably foreseeable.

103. It was therefore foreseeable that the failure to adequately safeguard Personally

Identifiable Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, causing monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, causing monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

104. For these reasons, Plaintiffs, individually and on behalf of all those similarly situated, seek an order declaring that Defendant's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND COUNT
Breach of Implied Contract
On behalf of Plaintiffs, the Class, and the State Subclasses

105. Plaintiffs re-allege and incorporate by reference preceding factual allegations found in paragraphs 1 through 91.

106. When Plaintiffs and Class Members paid money and provided their Personally Identifiable Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

107. Defendant solicited and invited prospective and current customers to provide their Personally Identifiable Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Personally Identifiable Information to Defendant.

In entering into such implied contracts, Plaintiffs and Class Members assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiffs and the Class Members to pay for adequate and reasonable data security practices.

108. Plaintiffs and the Class Members would not have provided and entrusted their Personally Identifiable Information to Defendant without the implied contract between them and Defendant to keep the information secure.

109. Plaintiffs and the Class Members fully performed their obligations under the implied contracts with Defendant.

110. Defendant breached its implied contracts with Plaintiffs and the Class Members by failing to safeguard and protect their Personally Identifiable Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

111. As a direct and proximate result of Defendant's breaches of its implied contracts, Plaintiffs and the Class Members sustained actual losses and damages as described here.

THIRD COUNT
Breach of Covenant of Good Faith and Fair Dealing
On behalf of Plaintiffs, the Class, and the State Subclasses

112. Plaintiffs re-allege and incorporate by reference preceding factual allegations found in paragraphs 1 through 91.

113. As described above, when Plaintiffs and the Class Members provided their Personally Identifiable Information to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' Personally Identifiable Information and to timely detect

and notify them in the event of a data breach.

114. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members were required to provide their Personally Identifiable Information in exchange for products and services provided by Defendants, as well as an implied covenant by Defendant to protect Plaintiffs' and Class Members' Personally Identifiable Information in its possession.

115. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their Personally Identifiable Information to Defendant but for the prospect of Defendant's promise of certain products and services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' Personally Identifiable Information if it did not intend to provide Plaintiffs and Class Members with the products and services it was offering.

116. Implied in these exchanges was a promise by Defendant to ensure that the Personally Identifiable Information of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon products and services.

117. Plaintiffs and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their Personally Identifiable Information in exchange for Samsung's implied agreement to keep it safe and secure.

118. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

119. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy

of the privacy and security protections for Plaintiffs' and Class Members' Personally Identifiable Information; storing the Personally Identifiable Information of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiffs and Class Members when they provided their Personally Identifiable Information to it that Defendant's data security systems failed to meet applicable legal and industry standards.

120. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

121. Likewise, all conditions required for Defendant's performance were met.

122. Defendant's acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

123. Plaintiffs and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personally Identifiable Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

124. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

125. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

FOURTH COUNT
Misrepresentation
On behalf of Plaintiffs, the Class, and the State Subclasses

126. Plaintiffs re-allege and incorporate by reference preceding factual allegations found

in paragraphs 1 through 91.

127. Defendant falsely represented to Plaintiffs and Class Members that it would take appropriate and reasonable measures to safeguard their Personally Identifiable Information.

128. Plaintiffs and Class members reasonably relied on said representations in that they provided Defendant their Personally Identifiable Information.

129. Defendant's misrepresentations were material, as Plaintiffs and Class Members would not have chosen to provide their Personally Identifiable Information to Samsung had they known that the information would be at heightened risk of compromise because of Samsung's lax data security.

130. As a result of Defendant's misrepresentations, Plaintiffs and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

FIFTH COUNT
Violation of the New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, et seq.
Plaintiffs, on behalf of the Class, and New Jersey Subclass

131. Plaintiffs re-allege and incorporate by reference preceding factual allegations found in paragraphs 1 through 91.

132. Plaintiffs and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

133. Defendant is a "person" as defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

134. Defendant's conduct as alleged related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

135. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of New Jersey.

136. Defendant solicited Plaintiffs and Class Members to do business and uniformly and knowingly misrepresented that by joining, their Personally Identifiable Information was safe, confidential, and protected from intrusion, hacking, or theft.

137. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Personally Identifiable Information, including by implementing and maintaining reasonable security measures.

138. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

139. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Personally Identifiable Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

140. Defendant failed to provide notice to Plaintiffs and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

141. Defendant's acts and omissions, as set forth evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

142. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members are required to expend sums to protect and recover their Personally Identifiable Information, have suffered and will continue to suffer injury, ascertainable

losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personally Identifiable Information, and thereby suffered ascertainable economic loss.

143. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

SIXTH COUNT
Illinois Personal Information Protection Act,
815 Ill. Comp. Stat. §§ 530/10(a), et seq.
Plaintiff, on behalf of the Illinois Subclass

144. Plaintiff Scott ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and re-alleges the preceding factual allegations found in paragraphs 1 through 91.

145. As a publicly held corporation that handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), Samsung is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

146. Plaintiff and Illinois Subclass Members' PII includes PII as covered under 815 Ill. Comp. Stat. § 530/5.

147. As a Data Collector, Samsung is required to notify Plaintiff and Illinois Subclass Members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

148. By failing to disclose the Samsung data breach in the most expedient time possible and without unreasonable delay, Samsung violated 815 Ill. Comp. Stat. § 530/10(a).

149. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive

Business Practices Act.

150. As a direct and proximate result of Samsung's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass Members suffered damages, as described above.

151. Plaintiff and Connecticut Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Samsung's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

SEVENTH COUNT
Illinois Consumer Fraud Act,
815 Ill. Comp. Stat. §§ 505, et seq.
Plaintiff, on behalf of the Illinois Subclass

152. Plaintiff Scott ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and re-alleges the preceding factual allegations found in paragraphs 1 through 91.

153. Samsung is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

154. Plaintiff and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

155. Samsung's conduct as described here was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

156. Samsung's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk

of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Violate common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and

disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

157. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

158. Samsung intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

159. The above unfair and deceptive practices and acts by Samsung were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

160. Samsung acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

161. As a direct and proximate result of Samsung's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described here, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the breach.

162. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

EIGHTH COUNT
Indiana Deceptive Consumer Sales Act,
Ind. Code §§ 24-5-0.5-1, et seq.
Plaintiff, on behalf of the Indiana Subclass

163. Plaintiff Rodriguez ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and re-alleges the preceding factual allegations found in paragraphs 1 through 91.

164. Samsung is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

165. Samsung is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

166. Samsung engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

167. Samsung's representations and omissions include both implicit and explicit representations:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

168. Samsung's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

169. The injury to consumers from Samsung's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

170. Consumers could not have reasonably avoided injury because Samsung's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Samsung created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

171. Samsung's inadequate data security had no countervailing benefit to consumers or to competition.

172. Samsung's acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Samsung's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Samsung's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Samsung concerning the state of Samsung security, and because it is functionally impossible for consumers to obtain credit without their PII being in Samsung's systems.

d. Because Samsung took unreasonable advantage of consumers' reasonable

reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

173. Samsung also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

174. Samsung intended to mislead Plaintiff and Indiana Subclass Members and induce them to rely on its misrepresentations and omissions.

175. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

176. Had Samsung disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Samsung would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Samsung was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. Samsung accepted the responsibility of protecting

the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on Samsung's misrepresentations and omissions, the truth of which they could not have discovered.

177. Samsung had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensively of the PII in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Samsung and Plaintiff and the Indiana Subclass as described herein. In addition, such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Indiana Subclass-and Samsung, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Samsung. Samsung's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

178. Samsung acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate. Samsung's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

179. Despite receiving notice, Samsung has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

180. Samsung's conduct includes incurable deceptive acts that Samsung engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

181. As a direct and proximate result of Samsung's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the breach.

182. Samsung's violations present a continuing risk to Plaintiff and Indiana Subclass Members as well as to the public.

183. Plaintiff and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

NINTH COUNT
Violation of the Michigan Identity Theft Protection Act Mich. Comp. Laws Ann. §§ 445.72, et seq.
Plaintiff Cole, on behalf of the Michigan Subclass

184. Plaintiff Cole ("Plaintiff" for purposes of this Count) re-alleges and incorporates by reference preceding factual allegations found in paragraphs 1 through 91.

185. Samsung is a business that owns or licenses computerized data that includes Personally Identifiable Information ("PII") as defined by Mich. Comp. Laws Ann. § 445.72(1).

186. Plaintiff's and Michigan Subclass Members' personal information includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

187. Samsung is required to accurately notify Plaintiff and Michigan Subclass Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

188. Because Samsung discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), Samsung had an obligation to disclose the Samsung data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

189. By failing to disclose the Samsung data breach in a timely and accurate manner, Samsung violated Mich. Comp. Laws Ann. § 445.72(4).

190. As a direct and proximate result of Samsung's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass Members suffered damages, as described above.

191. Plaintiff and Michigan Subclass Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

TENTH COUNT
Violation of the Michigan Consumer Protection Act Mich. Comp. Laws Ann. §§ 445.903, et seq.
Plaintiff, on behalf of the Michigan Subclass

192. Plaintiff Cole ("Plaintiff" for purposes of this Count) re-alleges and incorporates by reference preceding factual allegations found in paragraphs 1 through 91.

193. Samsung and Michigan Subclass Members are "persons as defined by Mich. Comp. Laws Ann. § 445.903(d).

194. Samsung advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

195. Samsung engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

196. representing that its goods and services have characteristics, uses, and benefits that they do not have;

197. representing that its goods and services are of a particular standard or quality if they are of another;

198. failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

199. making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and

200. failing to reveal facts are material to the transaction in light of representations of fact made in a positive matter.

201. Samsung's unfair, unconscionable, and deceptive practices include:

202. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Michigan Subclass Members' PII, which was a direct and proximate cause of the data breach;

203. failing to identify and remediate foreseeable security and privacy risks and

adequately improve security and privacy measures despite knowing the risks of cybersecurity incidents, which was a direct and proximate cause of the data breach;

204. violating common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

205. misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Michigan Subclass Members' PII, including by implementing and maintaining reasonable security measures;

206. misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

207. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Michigan Subclass Members' PII; and

208. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

209. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

210. Samsung intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

211. Samsung acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass Members'

rights. Samsung's March 2022 data breach put it on notice that its security and privacy protections were inadequate.

212. As a direct and proximate result of Samsung's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described here, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary to the breach.

213. Plaintiff and Michigan Subclass Members seek all monetary and on-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

ELEVENTH COUNT
Violation of the New Mexico Unfair Practices Act,
N.M. Stat. Ann. §§ 57-12-2, *et seq.*
Plaintiff, on behalf of the New Mexico Subclass

214. Plaintiff Sanchez ("Plaintiff," for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and re-alleges the preceding factual allegations found in paragraphs 1 through 91 as if fully set forth herein.

215. Samsung is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

216. Samsung was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

217. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, et seq., prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

218. Samsung engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce in violation of N.M. Stat. § 57-12-2, including the following:

a. Representing that its goods and services have approval, characteristics, benefits, or qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality when they are of another;

c. Using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive;

d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment;

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment.

219. Samsung's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4.

220. Samsung's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Samsung's data security and ability to protect the confidentiality of consumers' PII.

221. Samsung intended to mislead Plaintiff and New Mexico Subclass Members and induce them to rely on its misrepresentations and omissions.

222. Samsung acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass Members' rights. Samsung's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

223. As a direct and proximate result of Samsung's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Samsung's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the breach.

224. Plaintiff and New Mexico Subclass Members seek all monetary and non-monetary relief allowed by law, including pursuant to N.M. Stat. Ann. § 57-12-10, injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

TWELFTH COUNT
Declaratory and Injunctive Relief
Plaintiffs, on behalf of the Class

225. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as found in paragraphs 1 through 91.

226. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

227. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personally Identifiable Information it collected from Plaintiffs and Class Members.

228. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure their Personally Identifiable Information.

229. Defendant still possesses Plaintiffs' and Class Members' Personally Identifiable Information.

230. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

231. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Personally Identifiable Information in Defendant's possession is even more vulnerable to cyberattack.

232. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Personally Identifiable Information and Defendant's failure to address the

security failings that led to such exposure.

233. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

234. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third- party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data unnecessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their Personally Identifiable Information to third parties, as well as the steps they must take to protect themselves.

VI. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs and Class Members demand judgment as follows:

A. Certification of the action as a Class Action under Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representative and his counsel of record as Class Counsel;

B. That acts alleged above be adjudged and decreed to constitute negligence and violations of the consumer protection laws of Illinois, Indiana, Michigan, New Jersey, and New Mexico;

C. A judgment against Defendant for the damages sustained by Plaintiffs and the Classes above, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

1. Ordering that Defendant engage third-party security auditors/penetration testers as

well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

2. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

3. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

4. Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

5. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendant conduct regular database scanning and securing checks; and

7. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiffs and Class Members prejudgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after service of this Complaint;

F. The costs of this suit, including reasonable attorney fees; and

G. Any other relief that the Court deems just and proper.

VII. JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of all those similarly situated, request a jury trial, under Federal Rule of Civil Procedure 38, on all claims so triable.

DATED: September 26, 2022

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi
Caroline F. Bartlett
Jordan M. Steele
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
Facsimile: (973) 994-1744
jcecchi@carellabyrne.com
cbartlett@carellabyrne.com
jsteele@carellabyrne.com

Zachary S. Bower*
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
2222 Ponce DeLeon Blvd.
Miami, Florida 33134
Telephone: 973-422-5593
Facsimile: 973-994-1744
zbower@carellabyrne.com

Attorneys for Plaintiffs and the Proposed Class
** To be admitted pro hac vice*